Do Not Use the "%n" Format String Specifier

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03

L4 / D/P[4]

Careless use of "%n" format strings can introduce vulnerability.

Description

There are many kinds of vulnerability that can be caused by misusing format strings. Most of these are covered elsewhere, but this document covers one specific kind of format string vulnerability that is entirely unique for format strings. Documents in the public are inconsistent in coverage of these vulnerabilities.

In C, use of the "%n" format specification in printf() and sprintf() type functions can change memory values. Inappropriate design/implementation of these formats can lead to a vulnerability generated by changes in memory content. Many format vulnerabilities, particularly those with specifiers other than "%n", lead to traditional failures such as segmentation fault. The "%n" specifier has generated more damaging vulnerabilities. The "%n" vulnerabilities may have secondary impacts, since they can also be a significant consumer of computing and networking resources because large guantities of data may have to be transferred to generate the desired pointer value for the exploit.

Avoid using the "%n" format specifier. Use other means to accomplish your purpose.

References

[Hoglund 04]	Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code.* Boston, MA: Addison-Wesley, 2004.
[Newsham 00]	Newsham, Tim. *Format String Attacks*. http://www.lava.net/~newsham/format-string-attacks.pdf[10] (2000).
[scut 01]	scut. *Exploiting Format String Vulnerabilities*. http://julianor.tripod.com/teso-fs1-1.pdf (2001).
[Seacord 05]	Seacord, Robert C. *Secure Coding in C and C++*. Boston, MA: Addison-Wesley, 2005.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY

[3] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/320-BSI.html (Fithen, William L.)

[1] mailto:permission@sei.cmu.edu